Marquage de paquets

Netfilter et iproute

Documentation version 1.0 créé le 23 mai 2005
Dernière mise à jour le 20 juin 2005
Licence : GNU FDL
Copyright © : CRI74
Auteurs :
Emonet Jean-Bruno jbemonet@ext.cri74.org

Haute-Savoie
Centre de Ressources Informatiques
Bâtiment le Salève I
Site d'Archamps
F-74160 ARCHAMPS
Tél. : +33 (0)4 50 31 56 30
Fax : +33 (0)4 50 95 38 17
E-mail : info@cri74.fr
Web : www.cri74.fr
SIRET : 400 210 646 000 14
APE : 913 E
Le CRI dépend de l'Agence Économique Départementale - BP 2444 - F-74041 ANNECY CEDEX

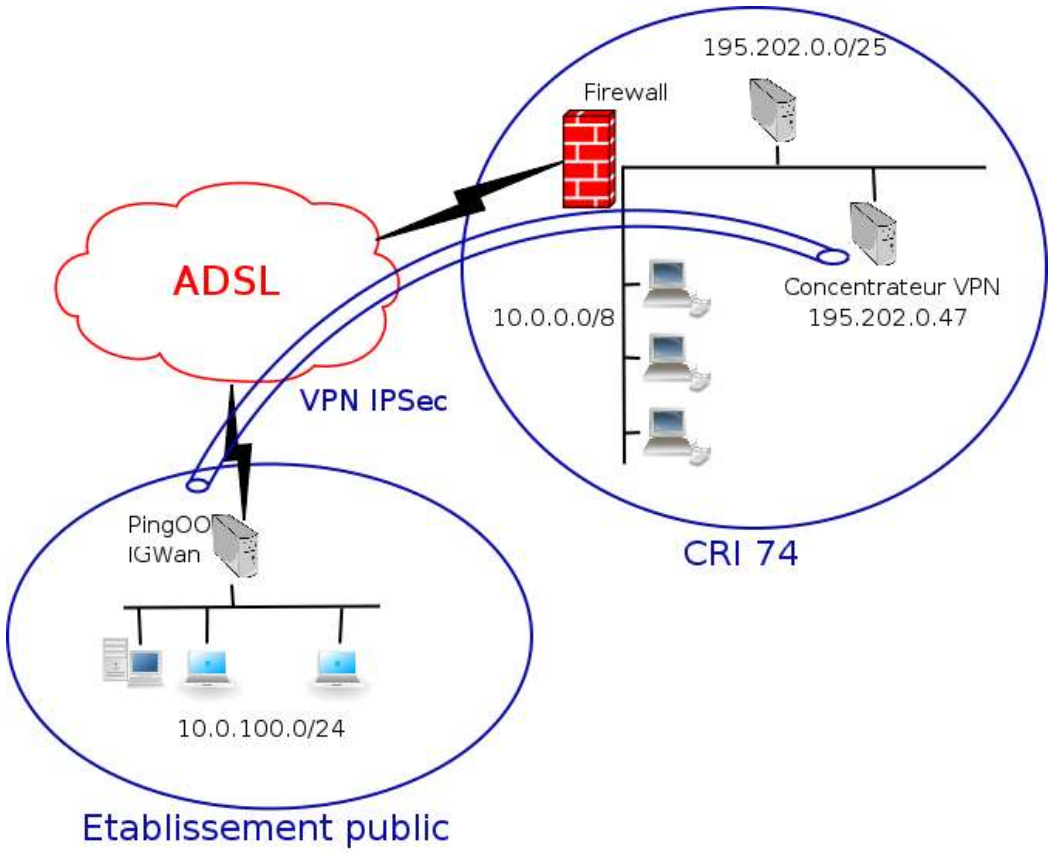
Table des matières

Copyright © CRI74 – GNU Free Documentation Licence

1 – Présentation

L' intérêt du marquage de paquets est de pouvoir différencier les paquets et les router de façon spécifique. Netfilter permet le marquage de paquets.

Ce marquage sera utiliser dans notre cas pour différencier les paquets qui ont empruntés le VPN et les autres. En effet, depuis le kernel 2.6 l'interface ipsec0 n'existe plus. Tous les paquets provenant du réseau et du VPN arrivent sur l'interface ppp0. Il faut donc filtrer ces paquets pour n'accepter par exemple que ceux qui proviennent du VPN.



1.1 – Configuration

Le VPN s'établit entre le réseau 10.0.100.0 de l'etablissement public et le réseau 195.202.0.0 du CRI74.

1.2 – Pré-requis

Pour le marquage de paquets avec Netfilter :

- vérifier l'activation des options suivantes dans le noyau dans Device drivers -->Networking Support --> Networking Support --> Networking Options

```
[*]IP: advanced router (CONFIG_IP_ADVANCED_ROUTER)
[*]IP: policy routing (CONFIG_IP_MULTIPLE_TABLES)
[*]IP: use netfilter MARK value as routing key (CONFIG_IP_ROUTE_FWMARK)
```

- Installer les paquetages iproute et iptables

Copyright © CRI74 – GNU Free Documentation Licence

2 – Configuration iptables

La configuration ne détaille que les règles pour permettre le marquage de paquets. Le reste dépend de votre configuration et de votre politique de sécurité.

2.1 – Client

2.1.1 – Table filter

INPUT

Tous les paquets marqués avec le chiffre 2 (par exemple) sont acceptés :

```
# iptables -A INPUT -i ppp0 -m mark --mark 2  -j ACCEPT
```

La tri peut-être plus restrictif en n'acceptant que les paquets ftp marqués :

```
# iptables -A INPUT -i ppp0 -m mark --mark 2 -p tcp -m tcp --dport 21 -j ACCEPT
```

Idem pour les connexions ssh :

```
# iptables -A INPUT -i ppp0 -m mark --mark 2 -p tcp -m tcp --dport 22 -j ACCEPT
```

2.1.2 – Table mangle

On marque les paquets entrants avec le chiffre 2 (c'est un exemple) provenant du réseau 195.202.0.0/24 utilisant le protocole esp(ex : VPN) :

```
# iptables -A PREROUTING -s 195.202.0.0/24  -i ppp0 -p esp -t mangle -j MARK --set-mark 2
```

2.2 – Serveur

2.2.1 – Table filter

INPUT

Tous les paquets marqués avec le chiffre 1 (par exemple) sont acceptés :

```
#  iptables -A INPUT -i eth0 -m mark --mark 1 -j ACCEPT
```

La tri peut-être plus restrictif en n'acceptant que les paquets ftp marqués :

```
#  iptables -A INPUT -i eth0 -m mark --mark 1 -p tcp -m tcp --dport 21 -j ACCEPT
```

2.2.2 – Table mangle

On marque les paquets entrants avec le chiffre 1 (c'est un exemple) à destination du réseau 195.202.0.0/24 utilisant le protocole esp(ex : VPN) :

```
#  iptables -A PREROUTING -d 195.202.0.0/24 -i eth0 -p esp -t mangle -j MARK --set-mark 1
```

Copyright © CRI74 – GNU Free Documentation Licence

3 – Webliographie

http://www.netfilter.org

http://www.lartc.org

http://www.linuxquestions.org/

http://christian.caleca.free.fr/netfilter/iptables.htm

http://www.freenix.fr/unix/linux/HOWTO/Advanced-routing-Howto-10.html

http://www.alaide.com/cours.php?c=6&chapter=752

http://www.linuxplusvalue.be/mylpv.php?id=64

http://www.linux-france.org/prj/inetdoc/guides/Advanced-routing-Howto/lartc.netfilter.html

Copyright © CRI74 – GNU Free Documentation Licence